Доклады семинара «Теория автоматов»

В третьем и четвертом кварталах 2018 года на научном семинаре «Теория автоматов» под руководством академика Валерия Борисовича Кудрявцева состоялось 11 докладов.

19 сентября 2018 года

Оптимизация аппаратных реализаций криптографических алгоритмов

аспирант Курганова Е. А.

В последнее время в сферах цифровой обработки сигналов, высокоскоростной передачи данных и криптографии все чаще возникает ситуация, когда программная реализация устройства не может обеспечить необходимую пропускную способность. Поэтому для многих современных цифровых устройств используются интегральные схемы. Помимо этого криптографические стандарты динамично меняются. Также из-за угрозы практической реализации квантовых вычислений в группу риска попадает подавляющее большинство стандартов с открытым ключом. В связи с этим возникает задача построения «криптографического конструктора», из которого можно оперативно порождать криптографические процессоры с эффективной поддержкой необходимой функциональности. Также с этой задачей неразрывно связана еще одна — создание кремниевого компилятора, т.е. программы, которая преобразует высокоуровневое описание алгоритма в схему в технологической библиотеке.

Аппаратные реализации моделируются схемами из функциональных элементов в расширенном базисе — конъюнкция, дизъюнкция, отрицание и задержка. Главным параметром производительности таких реализаций является глубина схемы, т.е. длина максимального простого пути схемы. Также в качестве дополнительного параметра часто рассматривают сложность — общее количество элементов схемы. И в том, и в другом случае элементы отрицания не учитываются при вычислении.

Первая часть доклада посвящена построению современных криптопроцессоров. Рассматриваются аппаратные реализации нескольких широко используемых симметричных шифров (DES, AES, ZUC, ГОСТ Р 34-12.2015), после чего производится сравнение скорости их работы. Приводится аппаратная реализация асимметричного шифра NTRUEncrypt,

обладающего устойчивостью к квантовым атакам, и кратко рассматривается реализация классического асимметричного шифра RSA. Данные реализации также сравниваются по глубине и сложности.

Во второй части доклада рассматривается построение аппаратных реализаций некоторых преобразований, часто используемых в криптографии. Приводится алгоритм для аппаратной реализации системы булевых функций, оптимизированной по сложности, а также результаты применения этого алгоритма к S-блокам (блокам подстановки).

19 сентября 2018 года

Свойства графов автоматов и других разложимых графов

аспирант Ищенко Р. А.

В докладе описываются свойства графов (диаграмм Мура) групповых и дефинитных автоматов, а также приводятся оценки хроматических чисел графов в зависимости от их толщины, охвата и древесности.

Автор рассматривает диаграммы Мура автоматов с точки зрения теории графов. В докладе рассказывается о критериях, позволяющих определить класс автомата по его диаграмме Мура, а также о том, в каких случаях ребра ориентированного графа можно разметить таким образом, чтобы образованная диаграмма Мура соответствовала групповому или дефинитному автомату. Приводятся описания алгоритмов, осуществляющих такую разметку.

Результаты во второй части доклада относятся к классической задаче теории графов: определению хроматического числа и других свойств графа в зависимости его разложения на более “простые” подграфы. В докладе приводятся оценки хроматического числа графа в зависимости от его толщины, охвата и древесности.

Доклад может быть интересен широкому кругу специалистов в теории автоматов и теории графов.

26 сентября 2018 года

Компьютерное моделирование логических процессов

профессор Подколзин А. С.

Главным средством изучения логических процессов на сегодняшний день является их компьютерное моделирование. Доклад посвящен исследованию техники такого моделирования. Это исследование позволило поднять уровень обучения компьютерных решателей задач до пограничного слоя между теоремами и алгоритмами и вплотную приблизиться к анализу источников саморазвития решателей. В процессе обучения возникла версия решателя, позволяющая не только получать ответ, но и показывать ход рассуждений по шагам.

3 октября 2018 года

Жизнь после описания сложности задачи удовлетворения ограничениям

с.н.с. Жук Д. Н.

В 2017 году была описана сложность задачи удовлетворения ограничениям на конечном множестве в зависимости от языка ограничений, что являлось основной открытой проблемой в данной области на протяжении 20 лет.

В докладе будет рассмотрен как этот результат, так и некоторые вариации и обобщения, которые до сих пор остаются открытыми проблемами и к которым сейчас приковано основное внимание. В частности, будет рассмотрено обобщение, где помимо кванторов существования допускаются также кванторы всеобщности (Quantified CSP), задача удовлетворения ограничениям на бесконечном множестве, задача удовлетворения ограниченям с обещанием (Promise CSP) и некоторые другие.

17 октября 2018 года

Решётка всех клонов на трёхэлементном множестве, задаваемых бинарными предикатами

Моисеев С. В.

В 2016-ом году автором была описана решётка всех клонов трёхзначной логики, которые могут быть заданы как классы сохранения некоторого множества бинарных предикатов. Оказалось, что существует ровно 2,079,040 таких клонов. В докладе будет рассмотрен этот результат, а также множество других фактов, выявленных в ходе работы над основным результатом.

24 октября 2018 года

О графовой модели криптографических протоколов

доцент Миронов А. М.

Криптографические протоколы — это распределенные алгоритмы, предназначенные для обеспечения безопасной передачи информации в небезопасной среде. Они используются, например, в электронных платежах, электронных процедурах голосования, системах доступа к базам данных, и т.д. Учитывая большой финансовый и социальный ущерб в случае неправильной работы таких протоколов, необходимо использовать математические методы для обоснования их корректности и безопасности. В докладе была предсталена новая математическая модель таких протоколов, позволяющая описывать как сами протоколы, так и их свойства. Было показано, как на базе данной модели можно решать задачи верификации криптографических протоколов.

31 октября 2018 года

Обучение устройств с дискретным управлением

аспирант Голиков К. А.

Сегодня во многих аспектах нашей жизни появляются автономные роботы, автомобили без водителя, самодвижущиеся устройства, дроны доставки, интеллектуальные алгоритмы, которые, обладая некоторыми

когнитивными функциями, для успешного взаимодействия с людьми, объектами и средой, должны уметь уточнять свою модель окружения в зависимости от меняющихся условий. В докладе будет рассмотрен один из подходов обучения систем и адаптации обучения к меняющимся условиям среды на примере задачи управления роботами с дискретным управлениям.

7 ноября 2018 года

О языках, устойчивых относительно операций выпадения, вставки

м.н.с. Дергач П. С.

В первой части доклада рассматривается два оператора замыкания языков — оператор вставки и оператор выпадения. Для них доказывается, что только регулярные языки могут быть замкнутыми. Приводится критериальное описание замкнутых классов в терминах регулярных выражений. Излагаются результаты об автоматной сложности таких языков. Решается проблема описания базисов возникающих классов, описываются все предполные классы, приводятся решения проблем полноты и выразимости.

Вторая часть доклада носит анонсирующий характер и посвящена переносу этих результатов на другие операторы замыкания. В частности, рассматривается оператор замыкания, заменяющий одну букву на две соседние, и обратный к нему. Приводятся некоторые результаты о свойствах возникающих замкнутых классов.

14 ноября 2018 года

О полиномиальной полноте конечных квазигрупп

с.н.с. Галатенко А. В.

Конечной квазигруппой называется конечное множество Q с бинарной операцией f такой, что для любых a и b из Q уравнения $f(x, a) = b$ и $f(a, y) = b$ однозначно разрешимы. Таблица Кэли квазигрупповой операции представляет из себя латинский квадрат. Квазигруппа называется полиномиально полной, если система из функции f и всех констант из Q полна относительно операции суперпозиции.

Одним из активно изучаемых приложений конечных квазигрупп является построение криптографических примитивов. При этом полиномиальная полнота — одно из желательных свойств, обеспечивающих стойкость. В докладе планируется рассмотреть критерии и алгоритмы проверки полиномиальной полноты.

21 ноября 2018 года

Распознавание лиц

с.н.с. Мазуренко И. Л.

В последние годы автоматическое распознавание лиц получило широкое применение на практике: эта технология работает в системах безопасности, используется для идентификации личности в мобильных телефонах, банковских системах, на транспорте, активно применяется в индустрии развлечений. В докладе будет дан обзор современного состояния науки и техники в этой области компьютерного зрения, а также приведены результаты совместной разработки по распознаванию лиц кафедры МаТИС и Московского исследовательского центра компании Хуавей. В завершающей части доклада будет сделана попытка формулировки сложных нерешенных математических и инженерных задач в области глубокого машинного обучения.

5 декабря 2018 года

Обобщенная реализуемость для языка арифметики и логики предикатов

м.н.с. Коновалов А. Ю.

Понятие реализуемости было введено в 1945 г. американским математиком С. К. Клини. В докладе предполагается рассмотреть модификации этого понятия, связанные с заменой в определении реализуемости класса всех частично-рекурсивных функций на другие классы функций.