

ПРОГРАММА
ХІХ Международной конференции
«ПРОБЛЕМЫ ТЕОРЕТИЧЕСКОЙ КИБЕРНЕТИКИ»
г. Казань, 28 сентября – 1 октября 2021 г.

Пленарные доклады

28 сентября

10.00 – 10.50

Алешин Станислав Владимирович (МГУ, Москва)

О трудах В. Б. Кудрявцева по математической кибернетике.

10.50 – 11.40

Аблаев Фарид Мансурович, Васильев Александр Валерьевич (КФУ, Казань)

Квантовое хеширование на состояниях высокой размерности

Аннотация. Ранее нами определена и исследовалась квантовая хеш-функция, обеспечивающая сбалансированное сочетание криптографических свойств в том числе благодаря применению так называемых "запутанных" состояний кубит. Создание запутанных квантовых состояний является сложной проблемой для современных квантовых технологий. При отказе от использования запутанных состояний удастся добиться такой же устойчивости к коллизиям лишь при отказе от устойчивости к восстановлению прообраза, что является одним из ключевых свойств криптографической хеш-функции. В связи с этим нами рассматривается реализация такой квантовой хеш-функции на основе состояний высокой размерности (так называемых "кудитов"), использующая совокупность незапутанных "кудитов".

11.40 – 12.30

Захаров Владимир Анатольевич (МГУ, Москва)

Алгебраический метод проверки эквивалентности для некоторых классов автоматов

Аннотация. Конечные автоматы-преобразователи, многоленточные автоматы, магазинные автоматы, биавтоматы - взаимосвязанные вычислительные модели, ведущие свое происхождение от концепции конечного автомата. Для автоматов из этих классов, обладающих свойством детерминированности или однозначности поведения, предложен универсальный метод построения быстрых алгоритмов проверки эквивалентности. Этот новый метод сводит задачу проверки эквивалентности автоматов к задаче проверки разрешимости систем уравнений над полукольцами языков или бинарных отношений. Как оказалось, такую проверку можно достаточно просто провести методом

исключения переменных, используя некоторые комбинаторные и алгебраические свойства регулярных префиксных языков.

29 сентября

10.00 – 10.50

Пережогин Алексей Львович (ИМ СО РАН, Новосибирск)

Спектры гамильтоновых циклов в булевом n -кубе

Аннотация. Спектром гамильтонова цикла в n -кубе называется кортеж из количеств ребер каждого направления, встречающихся в цикле. Дано полное описание всех спектров. А именно, доказана гипотеза Д.Кнута, что необходимые условия на спектр произвольного гамильтонова цикла являются достаточными для существования гамильтонова цикла с таким спектром.

10.50 – 11.40

Сергеев Игорь Сергеевич (НИИ "Квант", Москва)

Сложность линейных булевых операторов

Аннотация. В докладе рассказывается об основных результатах теории сложности линейных схем, реализующих булевы операторы (матрицы). Рассматриваются следующие виды схем: аддитивные схемы, вентильные схемы, схемы с операцией сложения по модулю. Приводится обзор методов получения верхних и нижних оценок сложности, а также результатов об экстремальных отношениях различных мер линейной сложности матриц.

11.40 – 12.30

Кочергин Вадим Васильевич (МГУ, Москва)

Задачи Беллмана и Пиппенджера и их различные вариации

Аннотация. С точки зрения сложности вычислений рассматриваются различные обобщения задачи о возведении в степень: задача Д.Кнута о вычислении набора степеней одной переменной, задача Р.Беллмана о вычислении одночлена общего вида, задача О.Б.Лупанова о вычислении элементов конечной абелевой группы по ее образующим, задача Н.Пиппенджера о вычислении систем одночленов. В качестве вычислительных моделей помимо классических схем из умножений рассматриваются схемы из умножений и делений, схемы из делений, схемы из умножений, допускающие использование величин, обратных к переменным, а также схемы композиции. Дается обзор как известных, так и новых результатов.

30 сентября

10.00 – 10.50

Алексеев Валерий Борисович (МГУ, Москва)

О некоторых фрагментах решетки замкнутых классов в частичной k -значной логике

Аннотация. Пусть A – замкнутый класс в k -значной логике P_k . В алгебре P_k^* частичных k -значных функций с операцией суперпозиции рассматриваются 3 типа фрагментов решетки замкнутых классов, порожденных классом A : 1) все замкнутые классы в P_k^* , содержащие A ; 2) все замкнутые классы в P_k^* , содержащие A , в которых множество всюду определенных функций совпадает с A ; 3) все замкнутые классы в P_k^* , содержащие A и состоящие только из функций, доопределимых до функций из A . В докладе дается обзор результатов по описанию таких фрагментов.

10.50 – 11.40

Кротов Денис Станиславович (ИМ СО РАН, Новосибирск)

О проблеме существования совершенных кодов и их обобщений

Аннотация. Совершенным код в дискретном метрическом пространстве эквивалентен разбиению пространства на шары фиксированного радиуса. Хорошо известна проблема существования совершенных кодов в пространствах, связанных с теорией кодирования. Для некоторых важных случаев (например, пространство Хэмминга над конечным полем, пространство матриц с ранговой метрикой) задача полностью решена, в то время как для других пространств (например, пространство Джонсона и пространство Хэмминга над неполовым алфавитом) она остается открытой, несмотря на значительные усилия исследователей. В докладе будут рассмотрены последние достижения в вопросах, связанных с существованием совершенных кодов и их обобщений, полностью регулярных кодов и трейдов, которые наследуют многие комбинаторные и алгебраические свойства совершенных кодов.

11.40 – 12.30

Часовских Анатолий Александрович (МГУ, Москва)

Полнота и выразимость в классах линейных автоматов.

Аннотация. В классе конечных автоматов с операциями композиции (суперпозиции и обратной связи) число предполных классов континуально [В.Б. Кудрявцев], а массовая задача проверки полноты конечных подмножеств алгоритмически неразрешима [М.И. Кратко]. Доклад посвящен классам линейных автоматов над конечными полями с операциями композиции. Для этих классов автором решена проблема полноты: найдены все предполные классы, что позволило получить алгоритм проверки полноты конечных подмножеств. В случае линейных автоматов над полем из двух элементов найдены замкнутые подклассы, содержащие сумматор. При естественных ограничениях решена задача аппроксимационной выразимости. Исследована структура предполных классов для линейных 2-адических автоматов с операциями композиции. Помимо методов

дискретной математики использован аппарат высшей алгебры: для полей Галуа и их трансцендентных расширений, колец, модулей над кольцами, линейных пространств.

1 октября

10.00 – 10.50

Mikhail Moshkov (KAUST, Er-Riyad, Saudi Arabia)

Complexity of Decision Trees over Infinite Systems of Attributes

Аннотация. In this presentation, we concentrate on the study of decision trees over infinite systems of attributes. We consider results obtained in the frameworks of two approaches: (i) the local approach in which in the decision trees solving a problem we can use only attributes from the problem description and (ii) the global one in which in the decision trees solving a problem we can use arbitrary attributes from the considered infinite system of attributes. We also briefly discuss a new direction of research related to the decision trees and based on the study of inference mechanisms for decision making.

10.50 – 11.40

Чашкин Александр Викторович (МГУ, Москва)

Об одном свойстве монотонных булевых функций

Аннотация. Установлено, что у любой n -местной монотонной булевой f функции найдутся две такие подфункции f_0 и f_1 , существенно зависящие от одних и тех же $n-k$ переменных, что $k > 1$, $f_0 \leq f \leq f_1$ и $f_0(x) < f_1(x)$ для $o(2^n)$ наборов x . Показано как можно использовать это свойство для вычисления значений монотонных функций.

11.40 – 12.30

Хадиев Камиль Равилевич (КФУ, Казань), Дмитрий Кравченко (университет Латвии, Рига), Yixin Shen (Лондонский университет, Лондон), Ремидовский Владислав (КФУ, Казань), Иликаев Артём (КФУ, Казань), Carlos Manuel Bosch Machado (КФУ, Казань)

Квантовые алгоритмы для обработки строк.

Аннотация. В докладе рассматривается набор задач по обработке строковых (текстовых) данных, для которых были построены квантовые алгоритмы, имеющие меньшее время работы, чем классические аналоги. Первая из задач - это задача распознавания языка Дика (правильной скобочной последовательности) константной глубины. Обсуждается квантовый алгоритм для случаев одного и нескольких типов скобок. Для обоих случаев алгоритмы демонстрируют квадратичное ускорение. Второй группой задач являются задачи конструирования текста из набора строк словаря. В частности, задача построения наименьшей общей суперстроки. Это задачи являющиеся близкими к задаче построения ДНК из составных частей (задачи секвенирования ДНК). Также рассматриваются важные базовые задачи, такие как задача сортировки строк и задача поиска наиболее частой строки в последовательности. В частности, известно, что нельзя построить квантовый алгоритм для сортировки чисел, работающий асимптотически быстрее

классических. В то же время, для сортировки строк ситуация другая, удалось построить квантовый алгоритм, работающий быстрее классических.