

# Доклады семинара «Вопросы сложности алгоритмов поиска»

В 2022 году на научном семинаре «Вопросы сложности алгоритмов поиска» под руководством профессора Эльяра Эльдаровича Гасанова состоялось 8 докладов.

7 сентября 2022 года

## **Параметро-эффективная расшифровка булевых функций**

м.н.с. Быстрыгова А. В.

В докладе 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).

14 сентября 2022 года

## **Число состояний клеточного автомата, реализующего двунаправленное движение на луче со скоростью движения вперёд $1/3$**

м.н.с. Кузнецова Е. В.

В докладе рассматривается движение точки на экране, который реализован, как клеточный автомат на бесконечной в правую сторону полосе шириной в одну клетку. Изучается класс  $S$  законов движения этого автомата, для которых движение вперёд возможно со скоростью, не большей, чем  $1/3$ . Движение вперёд на одну клетку осуществляется с двумя остановками. Возможно движение назад со скоростью 1, также точка может стоять на месте произвольное количество тактов.

Определён класс клеточных автоматов — толкатели. Ранее в классе толкателей реализованы законы движения со скоростью движения вперёд  $1/4$  и скоростью движения назад  $1/2$ , а так же законы движения со

скоростью движения вперёд  $1/3$ , скоростью движения назад 1 и чётным количеством остановок.

В данной работе доказано, что в классе толкателей невозможно построить клеточный автомат с количеством состояний, меньшим пяти, реализующий законы движения из рассматриваемого класса  $S$ . Результат получен для случая, когда до появления точки на экране все клетки находятся в состоянии покоя.

19 октября 2022 года

## **Верхняя оценка переключательной мощности плоских схем, реализующих один класс автоматов**

м.н.с. Воротников А. С.

Плоские схемы (или схемы из клеточных элементов) - это в некотором смысле укладка схемы из функциональных элементов на плоскость. Данные объект рассматривали многие авторы, в частности получен порядок потенциала и переключательной мощности для плоской схемы, реализующей булеву функцию от  $n$  переменных, составляющий  $2^{n/2}$ .

В данной работе рассматривается расширенное понятие: плоские автоматные схемы. Это схемы, чей базис клеточных элементов составляют, помимо привычных булевых функций с не более чем четырьмя входами и выходами, задержки — автоматы с одним состоянием, подающие на выход в следующий такт то, что пришло на вход в предыдущий. Корректные схемы теперь в каждом ориентированном цикле должны содержать не менее одной задержки. Функционирует данная конструкция как структурный автомат.

В работе показано, что некоторый класс автоматов можно реализовать плоскими автоматными схемами со средней переключательной мощностью на такт не более чем  $2^{n/2}/\log_2 n$ . Приводится схема с обозначенными параметрами.

9 ноября 2022 года

## **Распознавание автоматом свойства графа быть графом-кактусом**

асп. Демидова А. А.

Графом-кактусом является такой связный граф, в котором любое ребро принадлежит не более чем одному циклу (и любые два цикла могут иметь не более одной общей вершины). В работе рассматриваются автоматы, осуществляющие обход связных плоских простых неориентированных графов с целью определения того, являются ли эти графы графами-кактусами. Автомату доступно некоторое количество стираемых красок, которые он наносит на рёбра в течение обхода графа. Во время обхода автомат обладает частичной информацией о вершинах, которые он посещает, и инцидентных им рёбрах. В частности, в любой момент времени автомату известно, красил ли он только что некоторое ребро, благодаря чему он может обнаруживать циклы в графе. В работе исследуется возможность автоматов с 3 стираемыми красками оставлять на рёбрах такие метки, которые помогли бы установить, является ли граф кактусом или нет.

16 ноября 2022 года

## **Вопросы выразимости в классах кусочно-линейных функций**

доц. Миронов А. М.

В докладе представлены новая математическая модель криптографических протоколов и примеры применения этой модели для решения задач верификации криптографических протоколов. Криптографические протоколы — это распределенные алгоритмы, предназначенные для обеспечения передачи конфиденциальной информации в небезопасной среде. Они используются, например, в электронных платежах, электронных процедурах голосования, системах доступа к конфиденциальным данным, и т.д. Ошибки в криптографических протоколах могут привести к большому ущербу, поэтому необходимо использовать математические методы для обоснования различных свойств корректности и безопасности криптографических протоколов. В докладе изложены новые методы формальной верификации криптографических протоколов.

23 ноября 2022 года

## **Реализация сложения чисел клеточными автоматами и клеточными автоматами с локаторами**

проф. Гасанов Э. Э.

Было рассказано, как можно реализовать сложение натуральных чисел клеточными автоматами и клеточными автоматами с локаторами в одномерном и двумерном случаях.

30 ноября 2022 года

## **Нижняя оценка сложности расшифровки булевых функций веса 3 запросами на сравнение**

м.н.с. Быстрыгова А. В.

Рассматривается задача точной расшифровки запросами на сравнение булевых функций веса 3. Два игрока “учитель” и “ученик” играют в следующую игру. В начале игры учитель выбирает любую булеву функцию  $n$ -арности  $n$  веса 3. Ученик не знает выбор учителя, но знает  $n$ . Ученик последовательно задает запросы на сравнение, учитель на них безошибочно отвечает. Запрос на сравнение — упорядоченная пара  $n$ -местных наборов, ответ на запрос — разность значений выбранной учителем функции на этих наборах. Цель ученика — понять выбор учителя, задав как можно меньше запросов. В докладе представлено доказательство неулучшаемой нижней оценки этого количества.

7 декабря 2022 года

## **Алгоритм достижения консенсуса «Лотерея» и методы борьбы со злоумышленниками**

асп. Суюнбекова М. Б.

Рассматривается задача выбора одного игрока среди множества участников в качестве победителя, для решения которой приводится алгоритм “Лотерея”. Определяются классы злоумышленников, которые пытаются сорвать игру на основном этапе алгоритма. Для некоторых из этих классов приводятся протоколы их поимки.