# Доклады семинара «Вопросы сложности алгоритмов поиска»

В осеннем семестре 2019 – 2020 учебного года на научном семинаре «Вопросы сложности алгоритмов поиска» под руководством профессора Эльяра Эльдаровича Гасанова состоялось 14 докладов.

4 сентября 2019 года

## О прогнозировании сверхслов автоматами

асп. Ведерников И. К.

В докладе рассматривается задача прогнозирования сверхслов. Сперва вводятся основные классы автоматов, после чего доказывается, что наилучшая степень прогнозирования достигается в классе автоматов с размеченными функциями выхода. Затем приводятся критерий частичного прогнозирования общерегулярных сверхсобытий и критерий почти полного прогнозирования одноэлементных сверхсобытий. В конце доклада разбираются некоторые примеры иллюстрирующие перечисленные выше теоремы.

11 сентября 2019 года

## Оценки энергопотребления объёмных схем

асп. Ефимов А. А.

В ряде работ исследовалась сложность схем из функциональных элементов, реализующих функции алгебры логики от n аргументов. Автор использует такое понятие сложности схемы, как потенциал. Он равен среднему значению количества единиц на всех внутренних узлах схемы. Неформально говоря, потенциал играет роль средней «энергии» схемы, необходимой для её функционирования. Данная работа посвящена кубическим схемам, которые определяются аналогично плоским схемам, но в манхэттенском пространстве. Цель доклада состоит в получении верхней оценки потенциала объёмных схем, реализующих булевы функции и операторы из различных классов. Также целью является получение нижней оценки потенциала объёмных схем, из некоторого класса булевых операторов.

18 сентября 2019 года

## Об одном алгоритме перевода текста правил дорожного движения в формальную модель

асп. Менькин М. И.

Предлагается один из возможных подходов к автоматизированному переводу текста юридического документа в формальную модель на примере Постановления Правительства "О правилах дорожного движения". Перечислены основные сущности юридического документа, вводятся понятия графа дороги, дорожной ситуации, шаблона правила, синтаксического шаблона, разрешимости дорожной ситуации, в совокупности образующие формальную теоретико-графовую модель. Обозначены основные процедуры алгоритма перевода текста правил дорожного движения в данную модель. Приведены примеры разбора предложений, в которых идёт речь о манёвре "Уступить дорогу".

2 октября 2019 года

## Комбинаторно-геометрические свойства полиэдров задач комбинаторной оптимизации

д.ф-м.н. Максименко А. Н.

Примерами задач комбинаторной оптимизации с линейной целевой функцией являются задача о кратчайшем пути, задача коммивояжера, задача о рюкзаке и многие другие. Каждая такая задача может быть естественным образом переформулирована в виде задачи линейного программирования, область допустимых решений которой представляет собой выпуклый многогранник. С одной стороны, такая интерпретация позволяет использовать для решения этих задач геометрические методы. С другой стороны, и именно об этом и идет речь в докладе, этот подход позволяет выявить комбинаторно-геометрические свойства задач, характеризующие их сложность в различных классах алгоритмов. В докладе также рассмотрен метод аффинной сводимости, позволяющий сравнивать эти свойства.

9 октября 2019 года

## Расшифровка булевых функций из замкнутых классов Поста запросами на значение и запросами на сравнение

асп. Быстрыгова А. В.

В докладе рассматривается задача точной расшифровки функций из замкнутых классов Поста при помощи запросов на значение и запросов на сравнение. Приводится критерий возможности расшифровки запросами на сравнение. Показано, что для классов, которые возможно расшифровать запросами на сравнение, сложность расшифровки не хуже, чем таковая при использовании запросов на значение. Также приводятся примеры классов, для которых сложность расшифровки запросами на сравнение строго меньше сложности расшифровки запросами на значение.

16 октября 2019 года

## О конструировании клеточными автоматами двунаправленного движения на луче

студ. Кузнецова Е. В.

В докладе рассматривается вопрос числа состояний клеточного автомата, моделирующего движение точки на одномерном бесконечном экране. Приводится верхняя и нижняя оценка количества состояний данного клеточного автомата.

23 октября 2019 года

## Об одном алгоритме достижения консенсуса в криптовалютах

д.ф.-м.н., проф. Гасанов Э.Э, студ. Суюнбекова М.Б.

Предлагается новый алгоритм достижения консенсуса в криптовалютах. Алгоритм основан на выработке игроками совместного случайного числа, на основе которого определяется выигравший игрок. Вероятность выигрыша каждого игрока зависит от размера вложенных средств. При выработке совместного случайного числа каждый игрок обменивается информацией с некоторым числом игроков, и это число рано логарифму от общего числа игроков. Каждый обмен информации основывается

на протоколе "Подбрасывания монеты по телефону"Мануэля Блума. В отличии алгоритма достижения консенсуса, принятого в биткоин, предложенный алгоритм не требует существенных вычислительных ресурсов. Предложена схема организации блокчейна при данном алгоритме достижения консенсуса.

30 октября 2019 года

## Оценки кодового расстояния для классических и квантовых локальных кодов

к.ф.-м.н. Калачев Г. В.

В докладе рассматриваются семейства локальных кодов, исправляющих ошибки. Семейство локальных кодов — это семейство линейных кодов, заданных проверочной матрицей, у которых биты можно разместить в $D$-мерном пространстве таким образом, чтобы все биты, участвующие в одном проверочном соотношении, были расположены в шаре фиксированного радиуса. Известна верхняя оценка на кодовое расстояние и размерность $d$-мерных локальных кодов $d = O((n/k)^D)$.

В докладе рассмотрен пример кодов, где сообщение, заданное последовательностью из $2^t$ бит кодируется путём применения к нему одномерного линейного клеточного автомата Rule 60 $2^t$ раз. Закодированное слово состоит из всех состояний клеточного автомата в моменты $0, 1, ..., 2^t - 1$. Показано, что кодовое расстояние такого кода по порядку равно $3^t$, то есть $n^{(\log_2 3)/2}$, где $n \asymp 4^t$ — длина кодового слова.

Для аналогичных кодов, задаваемых другими линейными клеточными автоматами, порядок роста кодового расстояния неизвестен. Гипотеза заключается в том, что для любого линейного клеточного автомата эволюция одноклеточной конфигурации содержит минимальное по порядку количество клеток в состоянии 1.

6 ноября 2019 года

## Оценки кодового расстояния для некоторых семейств локальных квантовых кодов

к.ф.-м.н. Калачев Г. В.

В квантовых компьютерах все операции выполняются с определённой вероятностью ошибки, и поэтому для обеспечения надёжных квантовых вычислений необходимо защищать квантовое состояние. Для этого

предполагается использовать квантовые коды для коррекции ошибок. В докладе рассматриваются стабилизаторные CSS коды, задаваемые двумя проверочными матрицами $H_x$ и $H_z$ такими, что $H_x H_z^T = 0$. Особый интерес представляют локальные коды, у которых кубиты можно так разместить в $D$-мерном пространстве, чтобы все кубиты, участвующие в одном проверочном соотношении, были расположены в шаре фиксированного радиуса. Для вычисления синдромов локальных кодов требуются лишь локальные взаимодействия кубитов, поэтому такие коды более эффективны с точки зрения физической реализации.

Для квантовых LDPC кодов и, в частности, для локальных кодов лучшая известная оценка на кодовое рассояние $\Theta(\sqrt{n\sqrt{\log n}})$. Известно несколько семейств LDPC кодов, в том числе, локальных, у которых расстояние равно $\Theta(\sqrt{n})$. Для того, чтобы найти коды с более высоким расстоянием, требуется рассматривать другие классы кодов, для которых расстояние гипотетически может быть выше, чем $\sqrt{n}$. Есть гипотеза, что для 3-мерных фрактальных кодов может достигаться кодовое расстояние по порядку выше $\sqrt{n}$, однако для таких кодов лучшие известные нижние оценки $\Omega(\sqrt[3]{n})$. В докладе приведён пример кодов с фрактальной структурой ошибок, для которых удалось доказать нижнюю оценку $\Omega(n^\alpha)$, $\alpha = \log_2(2(\sqrt{5}-1))/3 \approx 0.435$. Также описаны задачи, связанные с клеточными автоматами, решение которых могло бы улучшить эту оценку. Среди них:

1) Оценка снизу числа единиц в эволюции линейного клеточного автомата Rule 150 на протяжении времени $2^t$, начиная с произвольного ненулевого состояния.

2) Рассматривается клеточный автомат Rule 150 со входом: у каждой клетки есть вход, на который можно подавать 0 или 1. Значение входа прибавляется к состоянию по модулю 2. Какое наименьшее число единиц (в сумме за всё время эволюции) нужно нужно подать на входы клеточного автомата, чтобы нулевое состояние через некоторое время перешло в состояние, где подряд $2^t$ клеток в состоянии 1?

13 ноября 2019 года

## Верхняя оценка мощности плоских схем, реализующих функции с ограниченным числом единиц

к.ф.-м.н. Калачев Г. В.

*Доклад состоялся в рамках первого заседания межфакультетского научного семинара "Актуальные математические задачи, связанные с проектированием СБИС" под руководством зав. кафедрой математической кибернетики факультета ВМК Ложкина С. А. и профессора кафедры МаТИС механико - математического факультета Гасанова Э. Э.*

Рассматривается задача синтеза плоских схем, реализующих булевы функции с ограниченным числом единиц плоскими схемами. $\mathcal{F}_n^N$ — класс всех булевых функций от $n$ переменных, принимающих значение 1 не более, чем на $N$ наборах. Из мощностных соображений можно убедиться, что площадь схем для почти всех функций не может быть меньше $N(n-\log_2 N)$ при $N \leq 2^{n-1}$. Кроме площади схем интерес представляет также энергопотребление, которому в модели плоских схем соответствует такая мера сложности, как потенциал. Потенциал схемы на входном наборе $x$ — это количество единиц в узлах схемы, когда на вход подан набор $x$. В докладе рассматривается максимальный потенциал схемы, равный максимуму потенциала по всевозможным входным наборам.

Приводится метод синтеза плоских схем, реализующих функции из $\mathcal{F}_n^N$ схемами с площадью $O(N(n-\log_2 N))$ и максимальным потенциалом $O(\sqrt{N(n-\log_2 N)n/\log_2 N})$. Сначала рассматривается случай $N \geq 2^{n/3}$, и строится схема с потенциалом $O(\sqrt{N(n-\log_2 N)})$. Затем рассматривается случай $N < 2^{n/3}$, и он сводится к последовательному вычислению $O(n/\log_2 N)$ функций от $3\log_2 N$ переменных, для которых используется схема, построенная на первом шаге, в итоге вся схема имеет требуемый потенциал.

20 ноября 2019 года

## О скорости роста одной колонии жуков

студ. Воротников А. С.

Рассмотрим следующую динамическу систему: дано бесконечное поле с ненулевым однородно расположенным запасом еды. На этом поле появляется жук, который перемещается по полю, ест имеющуюся еду и размножается. Поле моделируется целочисленной решёткой на плоскости,

в которой каждому узлу в начальный момент сопоставлено некоторое одинаковое количество еды. Эту целочисленную решётку в дальнейшем будем называть картой. Жук действует по алгоритму, который упрощённо представляется схемой: искать еду -> есть, пока не насытишься (если еды не хватило, снова искать) -> размножаться. На все действия расходуется энергия, которая получается жуком из еды, расположенной на поле. Если запас энергии жука падает ниже ноля, то жук умирает — исчезает с поля. Под размножением подразумевается деление жука на двух одинаковых жуков, обладающих половиной запаса энергии родителя.

Для некоторого класса прямых хочется построить класс колоний, такой, что для произвольной прямой найдётся колония, чей график численности бесконечное число раз пересекает выбранную прямую. Подзадача — описать такой класс прямых.

Указанная система моделируется однородными структурами. Предлагается использовать подход автоматного моделирования.

Сначала выбирается пять условий, которым должна удовлетворять колония, затем показывается, к каким ограничениям приводят эти условия. Далее следует анализ поведения жуков на карте, из которого вытекает необходимость корректировки некоторых условий. В результате непосредственного разбора поведения всех жуков, удаётся выписать явную функцию численности популяции с некоторого достаточно большого момента времени. Оказывается, что она лежит в конусе, ограниченном двумя прямыми, причём достигает границ конуса бесконечное число раз.

Таким образом удалось для произвольной прямой из класса

$$\mathcal{A} = \{y = ax + b | 0 < a \leqslant \frac{40}{11}, b \in \mathbb{R}\}$$

построить такую колонию, что её график численности популяции бесконечное число раз пересечёт выбранную прямую.

Обозначены требующие дальнейшего детального разбора способы расширения класса прямых до класса

$$\mathcal{B} = \{y = ax + b | a > 0, b \in \mathbb{R}\}.$$

27 ноября 2019 года

## Моделирование аэродинамики крыла клеточными автоматами

студ. Гордеева А. С.

В работе исследуется задача моделирования движения полета крыла в воздушном потоке. Предлагается для моделирования использовать клеточные автоматы. Причем считается, что имеются клеточные автоматы, моделирующие движение воздуха, и имеется автомат, моделирующий крыло. Крыло имеет некоторую форму. Клеточные автоматы изображают прямолинейное движение частиц, но при столкновении с крылом «обтекают» его, причем скорость частиц, движущихся по более длинной стороне крыла, больше чем у частиц с другой стороны. Из-за этого возникает подъемная сила. Автомат, моделирующий крыло, «видит» клеточные автоматы из некоторой окрестности крыла и высчитывает скорость частиц, их плотность. На основе этого вычисляется вектор подъемной силы. В результате крыло меняет свои координаты. Написана компьютерная программа, которая отображает функционирование предложенных автоматов. Проведены эксперименты с крыльями разных форм. Эксперименты показали адекватность модели.

4 декабря 2019 года

## Об асимптотически точных оценках сложности реализации булевых функций клеточными схемами и методах их получения.

д.ф.-м.н., проф. Ложкин С. А.

*Доклад состоялся в рамках второго заседания межфакультетского научного семинара "Актуальные математические задачи, связанные с проектированием СБИС" под руководством зав. кафедрой математической кибернетики факультета ВМК Ложкина С. А. и профессора кафедры МаТИС механико - математического факультета Гасанова Э. Э.*

В докладе представлен обзор результатов и методов, связанных с получением асимптотически точных оценок сложности реализации булевых функций и операторов в некоторых моделях клеточных схем из функциональных элементов и контактных схем.

11 декабря 2019 года

# Построение кратчайших путей клеточными автоматами с эхом.

д.ф.-м.н., проф. Гасанов Э. Э., студ. Пропажин А. А.

В докладе вводится новый объект — клеточный автомат с эхом. Каждый клеточный автомат с эхом в каждый такт может послать в эфир некоторый сигнал. Алфавит эфира является конечной аддитивной коммутативной полугруппой, а сам эфир представляет собой потенциально бесконечный сумматор сигналов клеточных автоматов, где в качестве суммы выступает определяющая операция данной полугруппы. В тот же такт каждый клеточный автомат получает из эфира суммарный сигнал и, учитывая его, изменяет свое состояние. Введение эфира и возможности посылать в эфир сигналы позволяет мгновенно передавать сигналы на любые расстояния, и тем самым позволяет одному клеточному автомату управлять поведением сколь угодно далеко удаленного от него другого клеточного автомата. Рассматривается также модификация клеточных автоматов с эхом, которые могут посылать сигналы в эфир по определенным направлениям и получать сигналы из эфира из определенных направлений. Иными словами, в этом случае у каждого клеточного автомата имеется несколько локаторов, направленных в разные стороны, и он может с помощью этих локаторов получать сигналы с определенных направлений и посылать сигналы по этим направлениям.

Исследуется задача поиска кратчайшего пути между двумя точками в среде с препятствиями. Приводится решение этой задачи с помощью клеточных автоматов с эхом. Проводится сравнение сложности решения этой задачи с помощью клеточных автоматов с эхом и с помощью обычных клеточных автоматов.