Московский государственный университет имени М. В. Ломоносова
Механико-математический факультет

Институт прикладной математики имени М. В. Келдыша РАН

ЧЕТЫРНАДЦАТЫЙ МЕЖДУНАРОДНЫЙ СЕМИНАР «ДИСКРЕТНАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ» имени академика О. Б. Лупанова (Москва, 20–25 июня 2022 г.)

Аннотации пленарных докладов

Гасанов Эльяр Эльдарович (Москва)
Клеточные автоматы с локаторами

В докладе будет представлен новый класс управляющих систем — клеточные автоматы с локаторами. Отличие клеточных автоматов с локаторами от клеточных автоматов состоит в том, что клеточные автоматы с локаторами могут посылать в эфир сигналы и получать из эфира суммарные сигналы. Такая возможность позволяет общаться автоматам, которые могут находиться сколь угодно далеко друг от друга. Будет показано как такие автоматы могут быть реализованы в виде физических устройств. Будет приведен ряд задач, которые в новом классе управляющих систем могут быть решены принципиально быстрее.

Грибанов Дмитрий Владимирович (Нижний Новгород)
Задача о подсчете целых точек в многограннике

Задача подсчета количества целых точек в произвольном многограннике, заданном системой линейных неравенств с целыми коэффициентами, является классической #**P**-трудной задачей. В 1993 году А. И. Барвинок показал, что данная задача может быть решена за полиномиальное время, если размерность объемлющего пространства является фиксированной. Ядром алгоритма А. Барвинка является эффективная процедура построения рациональных производящих функции простых конусов (под простым конусом мы понимаем d-мерный конус, порожденный d линейно-независимыми неравенствами). Эта процедура, в свою очередь, основана на идее построения знаковой декомпозиции исходного конуса в виде унимодулярных конусов.

Мы предлагаем альтернативный подход построения производящих функции, основанный на принципах динамического программирования и использующий периодичность структуры простых конусов. Отметим также, что мы строим более простые производящие функции, которые не содержат полной информации о целых точках внутри многогранника, но позволяющие вычислить количество этих точек.

Новый подход позволяет строить полиномиальные и псевдо-полиномиальные алгоритмы подсчета целых точек для различных классов многогранников произвольной размерности. К таким многогранникам, например, относятся дельта-модулярные симплексы, многогранники задач unbounded knapsack и multidimensional unbounded knapsack. Как одно из самых интересных приложений нового подхода, мы предлагаем новый алгоритм для задачи целочисленного линейного программирования с разреженной матрицей ограничений. Теоретическая оценка сложности нового алгоритма существенно превосходит оценку сложности лучшего из известных алгоритмов на классе задач с разреженными матрицами. Последний результат может быть использован для получения single exponential-time алгоритмов для задач мульти-упаковки/мульти-покрытия на графах/гиперграфах, например, таких как stable multiset и vertex multicover.

Евдокимов Александр Андреевич (Новосибирск)
О направлениях исследования и результатах по дискретному анализу в ИМ СО РАН им. С. Л. Соболева

Доклад предполагается состоящим из двух частей. В первой планируется рассказать об основных направлениях наших исследований в последние годы, включая вопросы кодирования структурированной информации, геометрии и комбинаторики вложений в n-мерные гиперкубы, метрические свойства дискретных пространств и криптографических булевых функций. В частности, кратко изложить результаты по дискретному анализу, вошедшие в важнейшие результаты ИМ СО РАН в последние годы.

Во второй части будет дано несколько определений параметрических отображений дискретных метрических пространств, сохраняющих, или частично искажающих, свойства близости и отделимости элементов. Эти отображения «ограниченного искажения» введены автором в 1988 году, а исследования продолжены в последующие годы, в частности, решены несколько задач о вложениях графов в гиперкубы в классе таких отображений. Это понятие и подход полезно, в частности, ассоциировать с дискретным вариантом непрерывности отображения и гомеоморфными вложениями, когда «близкие точки метрического пространства не разрываются, а далёкие точки не переводятся в близкие». Более широкая вариативность свойств отображений этого класса определяется выбором параметров близости и отделимости и будет проиллюстрирована на примерах.

Жук Дмитрий Николаевич (Москва)
Предикаты k-значной логики и задача удовлетворения ограничениям

В 1969 году была открыта удивительная связь между функциями и предикатами, а именно, было построено взаимно-однозначное соответствие между замкнутыми классами функций и замкнутыми классами предикатов. Несмотря на этот результат, многие годы именно функции были главным объектом исследований, а предикаты (отношения) оставались вспомогательным инструментом для описания предполных и замкнутых классов. В докладе будет представлен обзор результатов, полученных с помощью подхода, в котором основным объектом являются предикаты, а функции играют лишь вспомогательную роль.

Золотых Николай Юрьевич (Нижний Новгород)
Выделение эффективно разрешимых подклассов задачи целочисленного программирования

Хорошо известно, что задача целочисленного линейного программирования (ЦЛП) в общем случае **NP**-трудна. Все известные частные случаи полиномиальной разрешимости этой задачи можно разбить на две большие группы: задачи ЦЛП с фиксированным количеством переменных и задачи ЦЛП с ограниченными минорами. В докладе будет дан обзор результатов (полученных в том числе и представителями нижегородской школы дискретной математики), касающихся известных полиномиально разрешимых случаев этой и других близких задач.

Карпов Дмитрий Валерьевич (Санкт-Петербург)
Об изображениях на плоскости и раскрасках k-планарных графов

Граф называется k-планарным, если его можно так изобразить на плоскости, что каждое ребро пересекает не более чем k других. Наверное, впервые появилось такое обобщение в работе Рингеля в 1965 году — там были рассмотрены 1-планарные графы и доказано, что любой такой граф имеет правильную раскраску вершин в 7 цветов. Позже были определены k-планарные графы для всех натуральных k, исследовались вопросы об оценке на количество ребер в таких графах, оценке хроматического числа, различные вопросы об их изображениях на плоскости. В докладе будет рассказано о классических и современных результатах из этой области.

Колпаков Роман Максимович (Москва)
Некоторые проблемы комбинаторики слов

В докладе планируется дать обзор последних результатов, касающихся числа периодичностей, субпериодичностей и разрывных повторов в словах фиксированной длины. Под периодичностью (субпериодичностью) в слове понимается фрагмент слова, имеющий порядок (т.е. отношение длины слова к его минимальному периоду) не меньший, чем 2 (порядок меньший, чем 2). Разрывным повтором в слове называется пара одинаковых фрагментов слова с некоторым сравнительно небольшим разрывом между ними. Поиск и идентификация периодичностей, субпериодичностей и разрывных повторов имеет приложения для анализа и обработки текстовых и геномных данных, сжатия строковых данных.

Кочергин Вадим Васильевич (Москва)
Сравнение сложности вычисления одночленов и элементов конечных абелевых групп (сравнение оценок сложности для задач Р. Беллмана и О. Б. Лупанова)

В докладе планируется уделить внимание двум задачам. Первая из них заключается в исследовании сложности вычисления одночлена от m переменных, т. е. нахождения величины $l(x_1^{n_1}x_2^{n_2}\dots x_m^{n_m})$, определяемой как минимальное число операций умножения, достаточное для вычисления по переменным $x_1, x_2, \dots, x_m$ одночлена $x_1^{n_1}x_2^{n_2}\dots x_m^{n_m}$ (результаты промежуточных вычислений могут использоваться многократно). Эта задача сформулирована в 1963 г. Р. Беллманом и имеет интересную историю. Вторая задача, поставленная в 1988 г. О. Б. Лупановым, может быть определена как задача о сложности вычисления элемента $a_1^{k_1}a_2^{k_2}\dots a_m^{k_m}$ абелевой группы $\langle a_1\rangle_{u_1} \times \langle a_2\rangle_{u_2} \times \dots \times \langle a_m\rangle_{u_m}$ (предполагается, что $k_i < u_i$ для всех i). Понятно, что задачи Беллмана и Лупанова очень похожи и результаты, полученные для одной из них, как правило, переносятся на другую. Однако, в отдельных случаях значения сложности для этих задач могут и значительно отличаться. О сравнение значений сложности для задач Беллмана и Лупанова и пойдет речь в докладе.

Куликов Александр Сергеевич (Санкт-Петербург)
Нижние оценки для схем без ограничений: открытые задачи

Чтобы доказать, что классы **P** и **NP** различны, достаточно доказать суперполиномиальную нижнюю оценку на схемную сложность функции из **NP**. На данный момент мы бесконечно далеки от этого: не знаем, как доказать даже нижнюю оценку $4n$. Ещё более удручает тот факт, что методов для доказательства нижних оценок у нас тоже очень мало. В данном докладе мы обсудим несколько подходов, которые потенциально могут помочь улучшить известные нижние оценки на схемную сложность.

Купавский Андрей Борисович (Москва)
Случайные ограничения булевых функций и экстремальные задачи о пересечениях

Мы расскажем о новом подходе к приближению структуры семейств множеств, который дополняет уже существующий «метод дельта-систем» и «метод приближения хунтами». Подход, который мы называем разреженными приближениями, основан на понятии разреженных семейств и берёт начало в недавнем очень важном результате Альвайса и соавторов, получивших первое значительное продвижение в гипотезе Эрдеша-Радо о подсолнухах.

Общая идея подобных подходов к решению экстремальных задач состоит в следующем. Для данного комбинаторного объекта мы находим гораздо более простой объект, который хорошо его приближает с точки зрения экстремальной задачи и в идеале обладает такими же или похожими комбинаторными свойствами. Далее мы решаем экстремальную задачу в классе этих более простых объектов, и получаем, что если изначальный комбинаторный объект был экстремален, то он должен был приближаться экстремальным простым объектом. Последний шаг состоит в том, чтобы решить уже «локальную» задачу: если объект очень близок к предполагаемому экстремальному, то он должен с ним совпадать.

В этой методологии ключевым шагом является нахождение правильного класса «простых объектов» и количественные соотношения между их сложностью и качеством приближения. Напри-

мер, метод приближения хунтами подходит только для работы в достаточно «плотном» сценарии, когда экстремальные семейства составляют значительную часть от семейства всех множеств. В этом смысле наш подход очень гибок и позволяет работать и в сильно «разреженных» постановках.

Используя этот подход, мы получили значительные продвижения в нескольких классических задачах экстремальной комбинаторики, таких как задачи типа Алсведе-Хачатряна и Эрдеша-Шош для семейств множеств и семейств перестановок. Ранее в контексте перестановок использовалась очень сложная техника, основанная на анализе Фурье и теории представлений.

Доклад основан на совместной работе с Дмитрием Захаровым.

Ложкин Сергей Андреевич (Москва)
Уточненные асимптотические оценки сложности реализации булевых функций в некоторых классах схем

Около 25 лет тому назад появились первые так называемые асимптотические оценки высокой степени точности (АОВСТ) функций Шеннона $L(n), n = 1, 2, \ldots$, характеризующих сложность реализации «типичных» и самых «сложных» булевых функций от n переменных схемами из некоторых классов. Эти оценки позволяют установить поведение функции Шеннона $L(n)$ с относительной погрешностью $O\big(\frac{L(n)}{2^n}\big)$, тогда как известные ранее оценки имели относительную погрешность вида $O\big(\frac{L(n)}{2^n}\log\big(\frac{2^n}{L(n)}\big)\big)$. Иначе говоря, АОВСТ позволяют найти не только асимптотику самой функции Шеннона $L(n)$, но и асимптотику первого остаточного члена, а также порядок второго остаточного члена её «естественного» асимптотического разложения.

За прошедшее время АОВСТ и близкие к ним оценки были получены для большинства основных и ряда других классов схем, а также некоторых их частных случаев и модификаций. Были установлены АОВСТ функций Шеннона для сложности реализации булевых функций из некоторых специальных классов.

В докладе будет дан обзор указанных результатов, а также краткая характеристика основных приемов, используемых для их получения.

Перязев Николай Алексеевич (Санкт-Петербург)
О некоторых задачах теории мультиопераций

Мультиоперации это частичные многозначные функции от многих аргументов. Будут рассмотрены алгебры на множествах мультиопераций фиксированной размерности на конечных множествах с операторами суперпозиции и разрешимости, в частности, алгебры операций с оператором суперпозиции. В докладе будут представлены результаты о тождествах выполнимых в таких алгебрах, о соответствии Галуа для алгебр мультиопераций и алгебр операций, об описании минимальных алгебр в классе таких алгебр и некоторые другие задачи.

Райгородский Андрей Михайлович (Москва)
Графы, случайные графы и их экстремальные характеристики

В докладе планируется обсудить некоторые проблемы, связанные с раскрасками графов и их случайных подграфов, а также с различными смежными характеристиками, имеющими характер экстремальных: «размер максимальной клики в графе», «размер максимального независимого множества вершин», «минимальное число ребер в множестве вершин данной мощности» и т.д. Речь пойдет как о классических постановках в духе теорем Турана и Рамсея, так и о ряде новых вопросов, возникших в последние годы.

Смышляев Станислав Витальевич (Москва)
Методы теории сложности алгоритмов в криптографии

Доклад посвящен применению методов теории сложности алгоритмов в задачах обоснования положительных свойств безопасности криптографических механизмов и протоколов. Направление «доказуемой стойкости», развивающееся более 20 лет в международном научном сообществе, стало одной из основных тем, обсуждаемых на ведущих международных конференциях и симпозиумах по криптографии. Исследования в данной области направлены на построение теоретико-сложностных сведений задач нарушения безопасности сложных криптографических протоколов к сравнительно небольшому множеству стандартных задач для базовых объектов («примитивов»),

таких как блочный шифр, функция хэширования, эллиптическая кривая. В докладе будут рассмотрены основные принципы, определяющие данное направление исследований, а также будет приведен обзор используемого математического аппарата (естественным образом опирающегося на методы теории сложности алгоритмов). Кроме того, в качестве примеров будут рассмотрены некоторые результаты в данной области (в том числе, полученные автором), а также открытые задачи и актуальные направления исследований.

Федоряева Татьяна Ивановна (Новосибирск)

Типичные метрические свойства n-вершинных графов заданного диаметра

При изучении заданного класса графов, допускающих понятие размерности, т. е. меры их количества (часто под размерностью графа понимается число его вершин, разумеется, есть и другие подходы), естественно возникают вопросы асимптотического характера. При асимптотическом исследовании класса Ω_n графов размерности n особое внимание привлекает тематика вокруг следующих трех вопросов. Первый — вычисление асимптотически точного значения числа таких графов (или получение его хороших оценок). Это позволяет с установленной точностью достаточно просто подсчитать, как правило, трудно вычислимое число $|\Omega_n|$. Второй вопрос — выделение или построение подкласса типичных графов $\Omega_n^* \subseteq \Omega_n$ для заданного класса Ω_n. И третий — изучение общих, типичных свойств (справедливых для почти всех) рассматриваемых графов. Такой подход существенно помогает понять строение графов всего класса, особенно при большóм числе вершин.

В докладе обсуждается обозначенная тематика для класса n-вершинных графов заданного диаметра. Изучаются типичные метрические свойства этих графов, связанные с разнообразием метрических шаров, радиусом графа, диаметральными и центральными вершинами, центром графа и его спектром (множеством мощностей центров графов) и т.п., а также классы возникающих здесь типичных графов.

Чубариков Владимир Николаевич (Москва)

Деревья Хуа Ло-кена в теории сравнений по модулю, равному степени простого числа

Доклад посвящен изучению полиномиальных уравнений в целых p-адических числах. Описаны критерии, сводящие вопросы разрешимости таких уравнений к вопросам разрешимости сравнений по модулю степени простого числа.