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

Институт прикладной математики имени М. В. Келдыша РАН

Отделение Московского центра
фундаментальной и прикладной математики в МГУ имени М. В. Ломоносова

ПЯТНАДЦАТЫЙ МЕЖДУНАРОДНЫЙ СЕМИНАР «ДИСКРЕТНАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ» имени академика О. Б. Лупанова (Москва, 22–26 июня 2026 г.)

Предварительный список пленарных докладов

Сергеев Игорь Сергеевич (Москва)
Сложность вычислений в моделях схемного типа (обзор)

Обзор результатов о сложности вычислений в моделях схемного типа — в первую очередь, в моделях булевых и арифметических схем. Рассматриваются основные задачи и направления исследований. Акцент ставится на результатах и тенденциях последнего времени, а также на открытых проблемах.

Кочергин Вадим Васильевич, Михайлович Анна Витальевна (Москва)
Схемная сложность над бесконечными базисами (обзор)
Результаты с точными значениями сложности

В докладе планируется дать обзор известных результатов о сложности реализации булевых функций и функций многозначной логики схемами над бесконечными полными базисами. Кроме того, будут представлены новые результаты авторов, установивших точное значение схемной сложности для произвольной булевой функции при реализации над базисом, состоящим из всех монотонных булевых функций и отрицания, а также для произвольной функции k-значной логики над базисом, состоящим из всех монотонных относительно порядка $0 < 1 < \ldots < k-1$ функций и отрицания Поста.

Гасанов Эльяр Эльдарович, Калачев Глеб Вячеславович (Москва)
О вычислительных возможностях клеточных автоматов с локаторами

Клеточные автоматы с локаторами (КА с локаторами) расширяют классическую модель клеточного автомата механизмом широковещательного эфира: каждая ячейка может посылать сигнал из конечного алфавита, а принимать — сумму сигналов с заданных направлений, вычисленную с помощью заданной полугрупповой операции. В докладе рассматривается класс задач, решаемых двумерными КА с локаторами за логарифмическое время, и устанавливается его связь с известными классами сложности параллельных вычислений. В частности, показано, что задачи из класса NC^1 решаются КА с локаторами за логарифмическое время. Кроме того, показано, что класс задач, решаемых двумерными КА с локаторами за полиномиальное время, совпадает с PSPACE.

В докладе на идейном уровне будет рассказано, каким образом КА с локаторами решает задачи из схемных классов сложности в случае, когда описание схемы эффективно вычислимо. На первом этапе, исходя из длины входа, вычисляется размер схемы и подготавливаются начальные конфигурации для вычисления каждого элемента схемы. На втором этапе параллельно запускается моделирование машин Тьюринга с произвольным доступом из каждой подготовленной конфигурации; каждая машина вычисляет описание своего элемента схемы и номера элементов, к которым он подключён. На третьем этапе по вычисленным описаниям строится разметка на

плоскости, предназначенная для непосредственного моделирования схемы. На завершающем этапе автомат моделирует вычисление схемы на заданном входе.

Кроме того, будет кратко рассказано о моделировании самих КА с локаторами в других вычислительных моделях, что даёт оценки сверху на их вычислительную мощность.

Райгородский Андрей Михайлович (Москва)
О разбиениях множеств в пространствах

Речь пойдет о некоторых задачах на стыке комбинаторной геометрии, теории графов и теории кодирования. В контексте комбинаторной геометрии эти задачи активно исследовались в случае евклидовой метрики, а в последние годы появился ряд неожиданных результатов в случае метрик l_p, $p \neq 2$. Я расскажу про историю этой проблематики и про ее недавнее неожиданное развитие.

Аблаев Фарид Мансурович (Казань)
Эффективные квантовые алгоритмы поиска на основе техники хеширования

Дается обзор работ последних лет в области разработок квантовых алгоритмов поиска элемента в неупорядоченном наборе данных на основе техники хеширования, анализ их временной сложности и сложности памяти. Показывается, что применение техники квантового позволяет значительно сократить количество используемых кубит без увеличения запросной сложности.

Малышев Дмитрий Сергеевич (Нижний Новгород)
Алгоритмы векторного поиска: обзор и последние достижения

Поиск в большой векторной базе данных, который возвращает k векторов, наиболее близких к заданному вектору запроса, лежит в основе многих важных приложений, таких как компьютерное зрение, выдача рекомендаций и большие языковые модели. Для повышения эффективности векторного поиска на практике обычно используются приближенные алгоритмы, которые возвращают большинство из ближайших k соседей для каждого запроса. В докладе будет представлено введение в методы приближенного векторного поиска с некоторым акцентом на графовые алгоритмы. Кроме того, будут представлены новые библиотеки векторного поиска KBEST и KSCaNN, разработанные для новейших процессоров Huawei Kunpeng 920. Они в 1,6–2 раза превосходят по быстродействию известные современные алгоритмы векторного поиска, работающие на процессорах x86.

Вороненко Андрей Анатольевич (Москва)
Универсальные функции

В докладе рассматривается введенный автором (2012) объект — универсальные функции. Эти функции частью своих значений однозначно задают любую из функций, возможных в силу некоторого дополнительного ложного предположения. Для универсальных функций изучены вопросы существования, минимальной размерности области определения, наличия аналитического представления и возможные обобщения. Наиболее часто изучался класс линейных функций в силу наличия большого количества невырожденных постановок. Доклад сделан по материалам цикла, содержащего более 15 рецензируемых работ.

Чубариков Владимир Николаевич (Москва),
Михайлов Илья Петрович (Лениногорск)
О некоторых представлениях действительных чисел

В настоящем сообщении мы рассмотрим обобщение известной теоремы Харди–Литтлвуда (1914) о равномерном распределении последовательности остатков вида $x_n = x_n(\alpha) = \{q^n\alpha\}$ в q-ичном разложении почти всех действительных чисел α, где $q > 1$ — натуральное число, т.е. представление чисел $0 \leq \alpha < 1$ при $n \geq 1$ в следующей форме

$$\alpha = \frac{\lambda_1}{q} + \frac{\lambda_2}{q^2} + \cdots + \frac{\lambda_n}{q^n} + \frac{x_n}{q^n}, \quad \lambda_k = [qx_{k-1}], 1 \leq k \leq n, \quad x_n = \{qx_{n-1}\}, x_0 = \alpha.$$

В сообщении сформулированы теоремы о представлении действительных чисел α с помощью бесконечной итерации последовательности положительных монотонных функций $\alpha_n = f_n(x_n)$ в

виде

$$\alpha = \lambda_0 + f_1(\lambda_1 + f_2(\lambda_2 + f_3(\lambda_3 + \dots))),$$

где "цифры" $\lambda_n,\ n \geq 0$, и "остатки"

$$r_n = r_n(\alpha) = f_{n+1}(\lambda_{n+1} + f_{n+2}(\lambda_{n+2} + f_{n+3}(\lambda_{n+3} + \dots))),\ n \geq 0,$$

определяются по следующим рекуррентным формулам

$$\lambda_0 = [\alpha],\ r_0 = \{\alpha\},$$

$$\lambda_n = [\varphi_n(r_{n-1}(\alpha))],\ r_n = \{\varphi(r_{n-1})\},$$

причем $\{z\}$ и $[z]$ обозначают соответственно дробную и целую части действительного числа z и $x_n = \varphi_n(\alpha_n),\ n \geq 1$, — обратные функции для $\alpha_n = f_n(x_n)$.

В частности, представление числа α с помощью функции $f(x) = \frac{1}{x}$ приводит к цепной дроби для числа α. Общий случай, когда $f(x)$ — убывающая функция, был рассмотрен Б. Х. Биссинжером (1944) и А. Реньи (1957). Для функции $f(x) = \frac{x}{q}$ при $q \geq 2$ — натуральном числе получается q-адическое представление вида $\alpha = \sum \lambda_n q^{-n}$, где цифры $\lambda_n,\ n \geq 1$, могут принимать все целые значения от 0 до $q-1$. Случай возрастающей функции $f(x)$ исследовался С. И. Эвереттом (1946) и А. Реньи (1957). Представление α для $f(x) = \frac{x}{\theta}$ при нецелом $\theta > 1$ изучалось А. Реньи (1957) и А. О. Гельфондом (1959). В настоящей работе для последовательности функций $f_n(x) = \frac{x}{q_n}, q_n \geq 2$, — целые числа, исследуется представление α по мультипликативной системе чисел при $n \geq 1$ в виде

$$\alpha = \lambda_0 + \frac{\lambda_1}{q_1} + \dots + \frac{\lambda_n}{q_1 \dots q_n} + \frac{x_n}{q_1 \dots q_n},$$

где цифры λ_n могут принимать целые значения от 0 до $q_n - 1$. А. Х. Гияси (2007) обобщила теорему Гельфонда, касающуюся мультипликативной системы чисел. Пусть $\theta_n,\ n \geq 1$, — последовательность действительных чисел, каждое из которых больше единицы. Тогда любое действительное число $\alpha,\ 0 < \alpha < 1$, может быть представлено в форме $\alpha = \sum\limits_{k=1}^{n} \frac{\lambda_k}{q_1 \dots q_k} + \frac{x_n}{q_1 \dots q_n},\ n \geq 1$, где последовательность x_n остаточных членов определяется рекуррентно

$$x_0 = \{\alpha\},\ x_1 = \{\theta_1 x_0\}, \dots, x_n = \{\theta_n x_{n-1}\}, \dots,$$

и последовательность целых чисел λ_n определяется по правилу

$$\lambda_0 = [\alpha],\ \lambda_1 = [\theta_1 x_0], \dots, \lambda_n = [\theta_n x_{n-1}], \dots.$$

Иванов Александр Олегович, Тужилин Алексей Августинович (Москва)

Расстояние Громова–Хаусдорфа в теории графов и комбинаторной геометрии

Расстояние Громова–Хаусдорфа измеряет степень неизометричности метрических пространств: у изометричных пространств расстояние равно нулю, и чем более «непохожи» пространства друг на друга, тем это расстояние больше. Имеется много важных приложений расстояния Громова–Хаусдорфа, как в фундаментальной науке, так и в прикладных областях, например, при изучении скорости роста дискретных групп, в компьютерной графике и вычислительной геометрии, в теории распознавания образов, в робототехнике, и даже в космологии. В настоящем докладе мы обсудим ряд результатов авторов, показывающих, что расстояние Громова–Хаусдорфа неожиданно возникает и в задачах дискретной геометрии. Мы расскажем о том, как с помощью расстояния Громова–Хаусдорфа можно вычислить

- веса ребер минимального остовного дерева;
- число кликового покрытия и хроматическое число графа;
- наименьшее число частей, на которые можно разбить ограниченное метрическое пространство

так, чтобы диаметры частей были строго меньше диаметра исходного пространства (в евклидовом пространстве эта задача называется проблемой Борсука);
- наименьшую размерность пространства с манхеттенской метрикой, в которое можно вложить данное конечное метрическое пространство.

Черемушкин Александр Васильевич (Москва)
Строение сильно зависимых функций, удовлетворяющих функциональным тождествам

В докладе будет дан обзор результатов по описанию строения бинарных сильно зависимых функций, удовлетворяющих функциональным тождествам медиальности, парамедиальности, комедиальности, ко-парамедиальности, таранзитивности и почти ассоциативности. Будет рассмотрен также случай обобщенных тождеств, когда в записи тождества используются произвольные наборы бинарных операций, а также случай n-арных медиальных и парамедиальных сильно зависимых функций. В качестве одного из применений полученных описаний будет приведено расширение общей схемы протокола Диффи–Хеллмана, описанной в работе В. А. Артамонова и В. В. Ященко в 1994 году, на случай, когда стороны используют различные наборы операций, а также ее обобщение на случай произвольных степенных индексов, указывающих на порядок расстановки скобок в произведении.

Галатенко Алексей Владимирович (Москва)
Порождение конечных квазигрупп

В ряде приложений, например, из области криптографии, возникает потребность в квазигруппах большого порядка. Табличное задание квазигрупп в этом случае становится невозможным из-за избыточной сложности по памяти. Один из возможных подходов к понижению пространственной сложности — переход от табличного задания квазигрупповой операции к формульному. В докладе планируется рассмотрение двух констукций для порождения квазигрупп большого порядка: ортоморфизмов абелевых групп специального вида и правильных семейств функций.

Бахарев Александр Олегович (Новосибирск)
Постквантовая криптография

Квантовые вычисления — это быстроразвивающиеся область компьютерных исследований, которая ставит под угрозу современные стандарты асимметричной криптографии. А именно, алгоритм Шора и его модификации способны взломать используемые в настоящее время криптосистемы, основанные на задачах дискретного логарифмирования и факторизации, при наличии достаточно мощного квантового компьютера. В связи с этим последние десятилетия развивается направление постквантовой криптографии — криптографии, предположительно стойкой к атакам с использованием квантового компьютера. В докладе будут рассмотрены подходы к построению постквантовых криптосистем, основанные на геометрических решетках, кодах, исправляющих ошибки, и системах алгебраических уравнений. Также будут приведены задачи, на которых основана стойкость рассматриваемых криптосистем, и методы их анализа.

Ролдугин Павел Владимирович (Москва)
Применение конструктивных и вероятностных методов перечислительной комбинаторики в некоторых задачах, возникающих в области защиты информации

Долбилин Николай Петрович (Москва)
О двух проблемах в теории многогранников

Будут обсуждены две открытые проблемы о связи внутренней и внешней геометрий выпуклого трехмерного многогранника.

Одна из них — так называемая проблема Дюрера (1970 г., J. Shephard, Oberwofach, ранее была известна как фольклор) о существовании у выпуклого многогранника «хорошей» развертки. Суть проблемы: дан компактный выпуклый многогранник, можно ли разрезать его поверхность вдоль ребер так, чтобы она разворачивалась на плоскость в простой, то есть самонепересекающийся связный, многоугольник. Предположение о том, что такой разрез существует для любого выпуклого многогранника, называют именем А. Дюрера в связи с тем, что в своих исследованиях по

теории живописи этот великий художник, «Леонардо да Винчи Северного Возрождения», строит именно такие развертки для весьма сложных многогранников. Будет обсужден ряд результатов в этом направлении, а также выдвинута «Анти-Дюрер» гипотеза.

Другая проблема связана со знаменитой теоремой А. Д. Александрова «о существовании выпуклого многогранника с данной разверткой». Эта замечательная теорема явилась решением проблемы Вейля для полиэдральной метрики. В дальнейшем она послужила основой решения А. Д. Александровым проблемы Вейля в общем случае. Теорема Александрова описывает необходимые и достаточные условия на развертку, чтобы она была разверткой выпуклого многогранника. При этом многогранник единственен с точностью до конгруэнтности. Проблема состоит в том, как по развертке восстановить этот единственный многогранник. Это – - трудная проблема, к решению которой, по мнению А. Д. Александрова, принципиальных идей пока нет. Будут обсуждены частные случаи этой проблемы (мы называем их «гамильтоновы развертки») , а также рассказано о том, как восстановить многогранник по развертке, имеющей лишь 5 вершин положительной кривизны (этот результат получен совместно с М. И. Штогриным).

Ковалев Михаил Дмитриевич (Москва)
О математических моделях в инженерии и порождаемых ими вопросах, связанных с графами

Речь пойдёт о составленных из жёстких стержней, соединённых на концах шарнирами, устройствах. В инженерных науках ими занимаются в теории механизмов и строительной механике. Хотя для описания наиболее применимых простых механизмов достаточно традиционного понятия кинематической цепи, для описания строения более сложных устройств стали привлекаться графы. Они оказались необходимы при построении математических моделей таких устройств. При изучении этих моделей не только используется теория графов, но и возникают новые связанные с графами задачи.