Краткие аннотации докладов

среда, 16 декабря 2009 г.

- **Ю.В.Матиясевич.** «Десятая проблема Гильберта и модели вычислительных процессов»

  Аннотация:
  В докладе будет дан обзор разнообразных моделей вычислительных процессов, как используемых для доказательства неразрешимости 10-й проблемы Гильберта, так и тех, неразрешимость или универсальность которых была установлена на основе теоремы о диофантовости перечислимых множеств.

- **С.И. Адян.** «Точная квадратичная оценка длины вывода в одной системе подстановок Туэ»

  Аннотация:
  Мы рассматриваем систему подстановок слов в алфавите {a,b,c}, задаваемую следующими правилами: $a^2 \to bc$, $b^2 \to ac$, $c^2 \to ab$. Д. Хофбауэр и Й. Вальдманн доказали, что при любом начальном слове W любая цепочка вывода в этой системе обрывается за конечное число шагов. Из их доказательства можно получить только экспоненциальную верхнюю оценку длины вывода в зависимости от длины W. Был поставлен вопрос о существовании полиномиальной верхней оценки. Мы даём точную квадратичную оценку максимальной длины цепочек вывода в данной системе.

четверг, 17 декабря 2009 г.

- **А.А. Разборов.** «Алгебры флагов»

  Аннотация:
  Значительная часть экстремальной комбинаторики посвящена изучению вопроса о том, чему, при определённых предположениях, может быть равна плотность вхождений фиксированных комбинаторных объектов (таких, как графы, орграфы или гиперграфы) в большие неизвестные объекты того же типа. Используя сравнительно простые идеи и конструкции из логики, алгебры и теории меры, мы строим общую теорию, позволяющую рассматривать все такие задачи в рамках единого подхода, а также выделить несколько общематематических структур, неявно используемых в большинстве ранее известных аргументов. Ядром этой структуры служат специальные коммутативные алгебры, определяемые в терминах конечных моделей рассматриваемой теории первого порядка. В настоящем докладе я попытаюсь дать общее представление об этой теории, уделив при этом особое внимание полученным с её помощью конкретным результатам.

- **М.А. Всемирнов.** «Диофантово кодирование и обобщенные многочлены Кантора»

  Аннотация:
  При исследовании диофантовых задач иногда полезно рассматривать диофантовы кодировки, то есть биективные полиномиальные отображения из N^n на N. Типичным примером являются классические многочлены Кантора и их композиции. Достаточно давно известны и другие конструкции, основанные на многомерных аналогах многочленов Кантора. Однако вопрос о классификации таких отображений или даже вопрос о конечности их числа при фиксированном n

оказываются необычайно сложными. Даже при n=2 ответ известен только для многочленов степени не выше 4. (Гипотеза состоит в том, что для n=2 кроме многочленов Кантора других полиномиальных биекций нет.) При этом решение в известных случаях использует довольно неожиданную теорию чисел (например, теорему Линдеманна о трансцендентности). В докладе будет рассказано об имеющихся элементарных подходах к этой задаче и о случае кубических многочленов от трех переменных.

- **Л.Д. Беклемишев.** «Алгебра доказуемости и разреженная топология»

  Аннотация:
  В докладе будут рассмотрены два класса объектов, имеющих различную природу, но неожиданным образом аналогичные по своим свойствам. С одной стороны, так называемые алгебры доказуемости, возникающие при изучении свойств формальной доказуемости в арифметических теориях. С другой стороны, топологические пространства, наделённые одной или несколькими разреженными топологиями, то есть такими, что любое непустое подмножество X имеет хотя бы одну изолированную точку.

  Алгебра доказуемости формальной арифметической теории T представляет собой булеву алгебру Линденбаума для T, расширенную оператором D_0: L→L, сопоставляющим любому предложению A гёделевское предложение, выражающее непротиворечивость теории T+A. Ее естественным обобщением является алгебра, в которой наряду с оператором D_0 рассматриваются операторы n-непротиворечивости D_n, выражающие истинность всех доказуемых в T+A предложений с n переменами кванторов.

  Операторы D_0, D_1,… могут интерпретироваться как операторы на алгебре всех подмножеств данного множества X. Оказывается, что в случае, когда на алгебре множеств выполнены все тождества алгебры доказуемости, каждый из этих операторов естественным образом определяет некоторую разреженную топологию на X, для которой $D_n(A)$ есть множество всех предельных точек множества A.

  В докладе будут рассмотрены свойства соответствующих политопологических пространств и их связи с вопросами из теории доказательств, в частности вопрос о полноте топологических пространств относительно системы тождеств алгебр доказуемости.

пятница, 18 декабря 2009 г.

- **И.Г. Лысёнок .** «Квадратичные уравнения в свободном моноиде»

- **Э.А. Гирш.** «Оптимальные системы доказательств и алгоритмы (обзор)»

  Аннотация:
  Оптимальная система доказательств - система, доказательства в которой не более, чем в полиномиальное количество раз длиннее, чем в любой другой системе. Если к тому же доказательства могут быть переделаны из доказательств в другой системе за полиномиальное время, система называется p-оптимальной.

  Существование (p-)оптимальной системы доказательств для языка пропозициональных тавтологий (и многих других языков) является важным открытым вопросом теории сложности. Я. Крайичек и П. Пудлак (1989) показали связь этого вопроса с существованием оптимальной полуразрешающей процедуры для этого языка. Недавно Х. Монро (2009)

доказал отсутствие такой процедуры при некоторых дополнительных предположениях.

В последние годы отсутствие эффективной перечислимости (а значит, и подобного рода универсальных объектов) преодолевалось либо переходом к эвристическим вычислениям (когда имеется вероятностное распределение на входах и допустима ошибка с небольшой вероятностью), либо использованием небольшого количества битов неравномерной подсказки (единой для всех входов одной длины). В частности, С. Кук и Я. Крайичек (2007) показали наличие p-оптимальной системы доказательств с неравномерной подсказкой; докладчиком же (совместно с Д.М. Ицыксоном) получена оптимальная полуразрешающая эвристическая процедура для любого полиномиально моделируемого распределения, заданного на дополнении языка.

- **А.С. Куликов.** «О выпуклых мерах сложности»
(доклад по статье Pavel Hrubes, Stasys Jukna, Alexander Kulikov, Pavel Pudlak. On convex complexity measures. TCS, 2009.)

  Аннотация:
  Классическая нижняя оценка n^2 на размер формул для функции чётности f, доказанная В.М. Храпченко, может быть рассмотрена как некоторая мера сложности на подпрямоугольниках комбинаторного прямоугольника $f^{-1}(0) \cdot f^{-1}(1)$. Обобщая данный подход, мы вводим понятие выпуклых мер сложности. Мы доказываем верхнюю оценку $O(n^2)$ для всех мер сложности и показываем, что многие меры, использованные ранее для доказательства нижних оценок на размер формул, являются выпуклыми. Мы также доказываем квадратичные верхние оценки для некоторого класса мер, не обязательно являющихся выпуклыми.

- **В.В. Подольский.** «О некоторых классах пороговых булевых схем ограниченной глубины»

  Аннотация:
  Пороговой функцией называется булева функция f от n переменных, которая задается знаком целочисленного линейного многочлена p от этих переменных. Пороговой схемой называем схему, составленную из пороговых функций.

  Пороговые функции и схемы играют важную роль в теории сложности булевых схем. Одной из важнейших открытых проблем в этой области является доказательство того, что какая-либо явно заданная булева функция не может быть реализована пороговыми схемами глубины 2 полиномиального (от числа переменных) размера.

  Докладчиком (совместно с Кристоффером Хансеном) предложена серия новых типов булевых схем ограниченной глубины. Каждому типу схем сопоставляется класс всех булевых функций, реализуемых схемами полиномиального размера данного типа. Оказывается, что эти новые классы функций хорошо вписываются в известную иерархию классов, задаваемых пороговыми схемами ограниченной глубины. Мы исследуем соотношения между этими классами.

  Мы также рассматриваем вопрос о существовании явно заданной булевой функции, не принадлежащей одному из наших классов. Мы доказываем, что этот вопрос не сложнее сформулированного выше вопроса о сложности реализации булевых функций пороговыми схемами глубины 2. Мы надеемся, что решение нашего вопроса даст новую технику для решения этой известной открытой проблемы.

- **Д.М. Ицыксон.** «Структурная сложность вероятностных вычислений с ограниченной ошибкой»

  Аннотация:
  На данный момент для вероятностных вычислений с ограниченной ошибкой не известно теоремы об иерархии по времени, также не известно полных задач в классе BPP относительно детерминированных сведений. Основное препятствие – это отсутствие вычислимой нумерации вероятностных машин, которые удовлетворяют условию ограниченной ошибки. Хартманис и Хемачандра в 1986 году показали, что существует такой оракул A, что в классе BPP^A нет полных языков. Барак в 2002 году показал, что если существует полная задача в классе BPP относительно достаточно сильных детерминированных сведений, то существует и иерархии по времени. Лучший результат, связанный с иерархией по времени суперполиномиальный: Карпинский и Вербик показали, что BPTime[$n^{\log n}$] строго содержится в BPTime [2^{n^c}] для c>0.

  В серии работ (Барак 2002), (Фортноу, Сансанам 2004) и (Мелкебик, Первышев 2007) доказывается иерархия по времени для вероятностных вычислений с ограниченной ошибкой, использующих несколько битов (в лучшем результате используется всего один бит) неравномерной подсказки. Фортноу и Сансанам в 2004 году доказали теорему об иерархии по времени для эвристических алгоритмов, такие алгоритмы могут выдавать неверный ответ на маленькой доле входов. Первышев в 2007 году существенно упростил это доказательство.

  Докладчиком построена полная задача относительно детерминированных сведений по Тьюрингу и доказана теорема об иерархии по времени в классе AvgBPP, который состоит из распределенных задач (языка и полиномиально моделируемого распределения), которые можно решить за полиномиальное в среднем случае (в смысле определения Левина) время вероятностными алгоритмами с ограниченной ошибкой.